The Congruent Number Problem and Elliptic Curves

Harrison Schroeder

April 24, 2015

Abstract

This paper explores the congruent number problem, which asks which rational numbers are areas of triangles with rational side lengths. We define a rational non-zero number that is the area of a rational triangle as a congruent number and seek a method for determining if a number is congruent or not.

For some numbers such as 6 it is relatively simple to check that this is the area of a rational triangle, but as possible congruent numbers increase in size, it gets increasingly difficult to obtain via trial and error. Thus, we seek a more efficient method in determining if a number is congruent or not. The method of choice establishes a connection between congruent numbers and elliptic curves, an algebraic curve useful far beyond its apparent properties.

After describing some essential properties of the elliptic curve, such as the algebraic operations it respects and how to add points on the curve, we move into a discussion of the rank of an elliptic curve. As it turns out, the rank of the elliptic curve determines whether a number is congruent or not. After a brief discussion of linearly independence and torsion points, we describe a way to determine the rank of an elliptic curve.

After a brief discussion of the L-Series, which is connected to the rank of the elliptic curve, we connect the rank to the sides of a rational triangle via a bijective function. Finally, we state Tunnell's theorem. This theorem relies on the Birch-Swinnerton Dyer conjecture and states two conditions, the first being that a number is congruent. If the second condition is satisfied, then so is the first and vice-versa. We arrive at a somewhat straightforward algebraic computation using elliptic curves to determine if a number is congruent and thus the area of a rational triangle.

1 Introduction

Imagine a right triangle with rational side lengths a, b, c. We call such a triangle a rational triangle. Recall from elementary school math that the area, A, of such a triangle can be represented as:

$$A = \frac{1}{2}ab$$

Note that all rational triangles have rational area, but not all integers will be the area of some rational triangle. For example, suppose we have a $3, 4, 5$ triangle such that $A = 6$. Clearly $a, b, c, A \in \mathbb{Q}$. However, there is no rational triangle that can produce an area of 1. Figuring out which $A \in \mathbb{Z}$ have corresponding rational triangles is the subject of this paper.

Definition 1. A rational non-zero number is called a *Congruent Number*, n, if n is the area of a right triangle with rational side lengths.

By this definition, replacing the A in the above equation with our new variable n yields a formula for obtaining congruent numbers.

$$n = \frac{1}{2}ab$$

6, the congruent number stated in the introduction, is easily acquired with sides of $a = 3, b = 4$. However, not all congruent numbers are so easily found.

For instance, $n = 5$ is a congruent number with sides lengths of $a = 3/2$ and $b = 20/3$. This is not so obvious, but still somewhat possible to surmise. However, after just an increase of two orders of magnitude, we arrive at incredibly complicated side lengths. Take for example $n = 157$. The side lengths required to come up with this congruent number are

$$a = \frac{3803298487826435051217540}{411340519227716149383203} \quad \text{and} \quad b = \frac{41134051922771614938320 3}{21666555693714761309610}$$

two numbers which are remarkably difficult to acquire via trial and error.

Here, we will refer to the number of digits in the numerator as the *height* of sides a and b. Notice that $n = 5$, a congruent number with one digit, has side lengths with height of 2. For $n = 157$, a congruent number with 3 digits, $n = 157$, the height of the side lengths skyrockets to 25. If the height were bounded, then there would be finitely many possibilities to search. However, given the exponential increase in the height of the side lengths, it seems unlikely that height is bounded.

Hilbert's tenth problem of 1900 poses the question of if there exists a universal algorithm for solving equations in which only integer solutions are allowed. Such an algorithm does exist for the solution of first-order equations. However, in 1970, Yuri Matiyasevich proved the impossibility of obtaining a general solution. Thus, there is not a priori any guarantee that we can find a solution.

Fortunately, there exists a much easier way to determine whether or not n is a congruent number, and it exists by using a concept known as Elliptic Curves.

2 Elliptic Curves

Definition 2. An *Elliptic Curve* over a field, F, is a curve defined by an equation of the form

$$y^2 = x^3 + ax + b, \quad a, b \in F$$

This expression, together with a point $\mathcal{O}$, the point at infinity, comprises our definition of an elliptic curve.

Definition 3. The *point at infinity*, $\mathcal{O}$ is defined as the addition of any three points, such that

$$P + Q + R = \mathcal{O}.$$

The point at infinity is attained when the line connecting two points on an elliptic curve approaches ∞.

One necessary condition of elliptic curves is that the determinant, D, cannot be equal to 0. This ensures that every point is non-singular, or that the elliptic curve is smooth. This condition is expressed as:

$$D = -16(4a^3 + 27b^2) \neq 0.$$

Figure 1 shows the graph of an elliptic curve with the equation $y^2 = x^3 - 5x + 4$ over a field $\mathbb{Q}$. Note that $a = -5$, $b = 4$, so $D = 1088 \neq 0$.

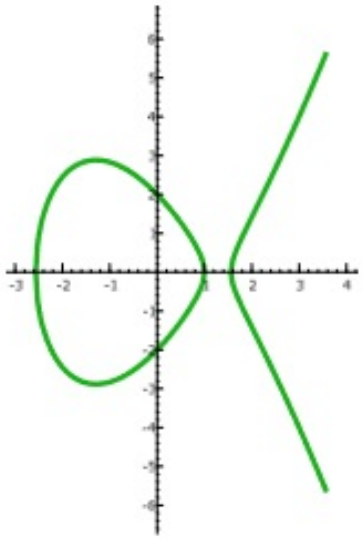

Figure 1: Elliptic Curve with equation $y^2 = x^3 - 5x + 4$
Accredited: William Stein

We denote such an elliptic curve over $\mathbb{Q}$, as

$$E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 - 5x + 4\} \cup \{\mathcal{O}\}$$

2.1 The Group Law

We can define the operation + on an Elliptic Curve by the following:

Definition 4. Geometric Group Law:
Let $P = (x_1, y_1), Q = (x_2, y_2) \in E(\mathbb{F})$, $x_1 \neq x_2$ and let L be the unique line through P and Q. Then, L intersects the graph of E at exactly one other point, $R = (x_3, y_3)$. The sum of P and Q is given by the inverse of R, or $(x_3, -y_3)$.

Proof.

$$\text{Set} \quad P = (x_1, y_1), Q = (x_2, y_2) \quad \text{and} \quad x_1 \neq x_2.$$

We calculate the slope, λ, by

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}.$$

Set the line from P to Q as

$$L_{PQ} : y - y_1 = \lambda(x - x_1)$$

Now, substitute y into $E(\mathbb{F})$ to get

$$(y_1 + \lambda(x - x_1))^2 = x^3 + ax + c.$$

To get a third point, R, we solve this equation. Group terms from left hand side by order of exponent of x

$$\lambda^2 x^2 + \lambda^2 x_1^2 + 2y_1\lambda(x - x_1) - 2\lambda^2 x_1 x + y_1^2 = x^3 + ax + b$$

We will only focus on the $\lambda^2 x^2$ term on the left hand side and the x^3 term on the right hand side. We will call the rest of the terms "lower x" such that

$$0 = x^3 - \lambda^2 x^2 + \text{"lower x"}$$

By the fundamental theorem of algebra,

$$0 = (x - x_1)(x - x_2)(x - x_3)$$

$$\text{So} \quad (x - x_1)(x - x_2)(x - x_3) = x^3 - (x_1 + x_2 + x_3)x^2 + \text{"lower x"}$$

$$\text{Thus} \quad x_1 + x_2 + x_3 = \lambda^2$$

$$\text{and} \quad x_3 = \lambda^2 - x_1 - x_2.$$

Now that we know x_3, we can define y_3 by the line

$$y_3 - y_1 = \lambda(x_3 - x_1)$$

$$y_3 = y_1 + \lambda(x_3 - x_1).$$

So, R has coordinates

$$P + Q = (x_3, -y_1 - \lambda(x_3 - x_1)) = (x_3, -y_3).$$

□

Example 5.

$E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 - 5x + 4\} \cup \{\mathcal{O}\}$. $P = (1, 0), Q = (0, 2)$. Compute $P+Q$.

$$\lambda = \frac{2 - 0}{0 - 1} = -2$$

$$x_3 = \lambda^2 - x_1 - x_2 = 4 - 1 - 0 = 3$$

$$y_3 = y_1 + \lambda(x_3 - x_1) = 0 - 2(3 - 1) = -4$$

$$P + Q = (x_3, -y_3) = (3, 4)$$

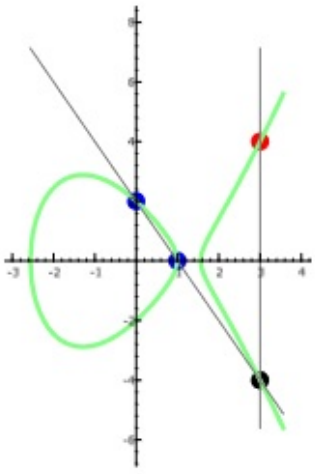

Figure 2: Visualization of adding points on Elliptic Curves
Accredited: William Stein

Note: When $P = (x, y)$ and $Q = (x, -y)$, $P + Q$ has a vertical tangent such that $P + Q = \mathcal{O}$.

Example 6.

$E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 - 5x + 4\} \cup \{\mathcal{O}\}$. $P = (0, 2), Q = (0, -2)$. Compute $P+Q$.

$$\lambda = \frac{-2 - 2}{0 - 0} = \infty$$

Thus, the slope of the line is vertical, which means $P + Q = \mathcal{O}$.

Note: For $P = (x_1, y_1)$ to add $P + P$, we use for λ the slope of the tangent line. To do so, we calculate $\frac{dy}{dx}$ from $y^2 = x^3 + ax + b$.

$$(2y)\frac{dy}{dx} = 3x^2 + a$$
$$\frac{dy}{dx} = \frac{3x^2}{2y} + \frac{a}{2y}$$
$$\frac{dy}{dx} = \frac{3(x_1)^2}{2y_1} + \frac{a}{2y_1} = \frac{3(x_1)^2 + a}{2y_1}.$$

Example 7.

$E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 - 25x\} \cup \{\mathcal{O}\}$. $P = (-4, 6)$. Compute $2P$.

$$\frac{dy}{dx} = \frac{3(-4)^2 - 25}{2(6)} = \frac{48 - 25}{12} = \frac{23}{12} = \lambda$$
$$x_3 = \lambda^2 - x_1 - x_2 = \frac{23}{12}^2 + 4 + 4 = \frac{1681}{144}$$
$$y_3 = y_1 + \lambda(x_3 - x_1) = 6 + \frac{23}{12}(\frac{1681}{144} + 4) = \frac{62279}{1728}$$
$$2P = R = (x_3, -y_3) = (\frac{23}{12}, \frac{-62279}{1728})$$

Theorem 8. *$E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$ is an abelian group. That is, it satisfies the following properties.*

1) $P + \mathcal{O} = P, \quad \forall P \in E.$

2) $\exists P_{inv} \in E : P + P_{inv} = \mathcal{O}.$

3) $(P + Q) + R = P + (Q + R), \quad \forall P, Q, R \in E.$

The proof of associativity on E is quite extensive and beyond the scope of this paper, but the proofs of the identity element and the inverse element are as follows.

Proof. Identity

To show that the point at infinity, $\mathcal{O}$, is the identity element on E, we appeal to the geometric definition of addition on E. Connect a line between $\mathcal{O}$ and a point $P = (x, y)$. Then, continue that line such that it intersects another point on E, $Q = (x, -y) = (x_3, y_3)$. Note that we defined addition of two points as $P + Q = (x_3, -y_3)$, and note that $(x_3, -y_3) = (x, y) = P$, then $P + \mathcal{O} = P$. □

Proof. Inverse

The inverse is defined as a point, P_{inv} on E such that $P + P_{inv} = \mathcal{O}$. If $P = (x, y)$, then clearly $P_{inv} = (x, -y)$. Thus, as shown in example 5, $\lambda = \frac{-y - y}{0 - 0}$, which yields a vertical tangent line, and $P + P_{inv} = \mathcal{O}$. □

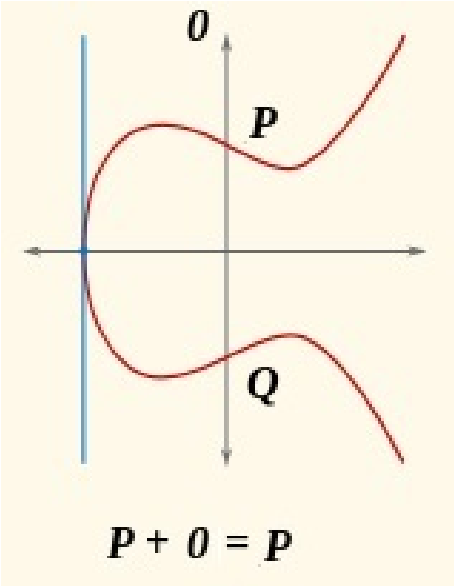

Figure 3: The Identity Element on E

Definition 9. If $P+P+\ldots+P = nP = \mathcal{O}$ for some nonzero $n \in \mathbb{Z}$, we say that P is *torsion*. Otherwise, the point is non-torsion. It can be shown that if $E(\mathbb{F})$ is finitely generated, then the sub-group $E(F)_{tor}$ must be finitely generated.

Theorem 10. *(Lutz-Nagell)*
If $E : y^2 = x^3 + ax + b$, $a, b \in \mathbb{Z}$, *then* $\mathcal{O} \neq (x, y) \in E(\mathbb{F})_{tors}$ *must satisfy*
1) $x, y \in \mathbb{Z}$
2) $y^2 \mid 4a^3 + 27b^2$

While this does not definitively tell us how to find points of torsion, this restricts possible torsion points.

Theorem 11. *Torsion Theorem for E*
Suppose $\exists p$ *a prime with* $p \nmid D = -16(4a^3 + 27b^2), a, b \in \mathbb{Z}$ *for some* $E(\mathbb{Q}) = \{(x, y) : y^2 = x^3 + ax + b\}$.
Then the map:

$$\pi : E(\mathbb{Q})_{tors} \to E(\mathbb{F}_p)$$

$$(x, y) \to (x \mod p, y \mod p)$$

$$\mathcal{O} \to \mathcal{O}$$

is an injective group homomorphism.

Proof. It is well-known by the Lutz-Nagell Theorem that all points of $E(\mathbb{Q})_{\text{tors}}$ have integer coordinates. So, reduction $\mod p$ makes sense.
It is know that when $p \nmid D$, $D \not\equiv 0 \mod p$ and $E(F_p)$ is also a group with the same addition law.
Now, since π is well-defined, only $\pi(\mathcal{O})$ goes to $\mathcal{O}$.
Thus:

$$(x, y) \in E(\mathbb{Q})_{tors} \leftrightarrow y^2 = x^3 + ax + b$$

and

$$(x, y) \in E(\mathbb{Q})_{tors} \leftrightarrow \bar{y}^2 = \bar{x}^3 + a\bar{x} + b$$

where $\bar{x} = x \mod p$ and $\bar{y} = y \mod p$.
To compute $P + Q, P, Q \in E(\mathbb{Q})_{tors}$, we solve for λ.

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = y_1 + \lambda(x_3 - x_1)$$

$$\lambda = \frac{3x_1^2 + a}{2y_1} \quad \text{if} \quad P = Q; \quad \lambda = \frac{y_1 - y_2}{x_1 - x_2} \quad \text{if} \quad x_1 \neq x_2$$

$$\pi(P), \pi(Q) \neq \mathcal{O} \in E(F_p); \quad P + Q = (x_3, -y_3) \in E(\mathbb{Q})_{tors}$$

$$\text{If} \quad \lambda \notin \mathbb{Z} \quad \text{then} \quad \lambda^2 - x_1 - x_2 = x_3 \notin \mathbb{Z}.$$

This contradicts Lutz-Nagell, so x_3, y_3 are also integers. So, λ makes sense in $E(F_p)$ for adding $\pi(P) + \pi(Q)$ and

$$\pi(P) + \pi(Q) = \pi(P + Q)$$

So π is a homomorphism.
Now we will show π is injective.

$$\text{Let} \quad \pi(P) = \pi(Q)$$

$$\text{Then} \quad \pi P - \pi Q = \mathcal{O}; \quad \pi(P - Q) = \mathcal{O}$$

Since only $\pi(\mathcal{O})$ maps to $\mathcal{O}$, we say:

$$P - Q = \mathcal{O}, \quad \text{and} \quad P = Q.$$

So, π is injective. □

Definition 12. Denote E_n as the elliptic curve $y^2 = x^3 - n^2x$ over $\mathbb{Q}$.

If K is a field whose characteristic p does not divide $2n$, then E_n is an elliptic curve over K. We let $E_n(K)$ denote the set of points on the curve with coordinates in K.

Theorem 13. *For $p \equiv 3 \mod 4$, $\#E_n(F_p) = p + 1$.*

Proof. In order to complete this proof, it is first necessary to prove some lemmas.

In F_p, $\frac{p-1}{2}$ numbers are non-zero squares (also called quadratic residues) and $\frac{p-1}{2}$ are not, with the last number is $\mathcal{O}$.
Why this is the case can be shown using primitive roots.

Lemma 14. *The group of units $F_p^\times$ is cyclic.*

Proof. We will demonstrate there exists an element of exact order $p-1$ that is a primitive root $\mod p$. It will follow that $F_p^\times$ is generated by this primitive root.
The primitive roots of $F_p^\times$ have exact order $x^{p-1} - 1 = 0$.
Note, for $p = 2$, 1 is a primitive root, so we assume that $p > 2$.
Write $p - 1$ as a product of distinct prime powers:

$$p - 1 = q_1^{n_1} q_2^{n_2} \dots q_r^{n_r}$$

It can be shown that the polynomial $x^{q_i^{n_i}} - 1$ where $q_i^{n_i} \mid (p-1)$ has exactly $q_i^{n_i}$ roots and $x^{q_i^{n_i}} - 1$, has exactly $q_i^{n_i - 1}$ roots.[1]

Then, there are $q_i^{n_i} - q_i^{n_i-1} = q_i^{n_i-1}(q_i - 1)$ roots $a \in F_p^\times$ such that $a^{q_i^{n_i}} = 1$, but $a^{q^{n_i-1}} \neq 1$, so each of these a have exact order $q_i^{n_i}$.

Thus, for each $i = 1 \dots r$, we can choose a_i that has exact order $q_i^{n_i}$. It can be shown[2] that

$$a = a_1 a_2 \dots a_r$$

has exact order $q_1^{n_1} q_2^{n_2} \dots q_r^{n_r} = p - 1$, thus a is a primitive root $\mod p$. □

Now, we can express

$$F_p^\times = \{1, g, g^2, \dots, g^{p-2}\} \mod p$$

for some g a primitive root.
If $a \equiv b^2 \mod p$, and $b \equiv g^k \mod p$, which it must be for some k, then

$$a \equiv b^2 \equiv (g^k)^2 \equiv g^{2k} \mod p$$

If $a \not\equiv b^2$ for any b, then $a = g^l$ for some l.
Since l is not of the form $2k$, then l must be odd.

[1] The proof of this statement can be found in William Stein's Elementary Number Theory, Proposition 2.5.5
[2] Lemma 2.5.7 in Stein

So, the even exponents of g are all squares, and the odds are not, so $\frac{p-1}{2}$ roots are even in $\mathbb{Z}/_{(p-1)}\mathbb{Z}$ and $\frac{p-1}{2}$ roots are odd in $\mathbb{Z}/_{(p-1)}\mathbb{Z}$, giving the result.
To prove that $\#E_n(F_p) = p+1$ when $p \equiv 3 \mod 4, p \nmid D$, we need to break up $F_p^\times$ into two categories, those that are squares and those that are not squares. This will separate the elements of $F_p^\times$ into those with two roots and those with zero roots.
We show that -1 is a square $\mod p$ if and only if $p = 1 \mod 4$. If -1 is not a square when $p = 3 \mod 4$, then we can break up $F_p^\times$ into $x's$ and $-x's$.

Proposition 15. *-1 is a square if and only if $p = 1 \mod 4$.*

Proof. Suppose -1 is a square. Then -1 is a root of $x^2 \equiv 1 \mod p$. The only other root is $g^{p-1} \equiv 1 \equiv g^0 \mod p$.
Every $x \in F_p^\times$ has a unique exponent $k \mod (p-1)$ with $g^k \equiv x$.
Let

$$-1 \equiv g^k \mod p \quad (k \not\equiv 0 \mod p-1)$$

Then

$$(-1)^2 \equiv g^{2k} \equiv 1 \equiv g^0 \mod p$$

$$2k \equiv 0 \mod (p-1)$$

$$k \equiv \frac{p-1}{2} \mod (p-1)$$

Since $p-1$ is even, this works. It is unique since -1 is defined as the root of $x^2 - 1$. Thus,

$$-1 \equiv g^{\frac{p-1}{2}} \mod p$$

Since, -1 is a square, call it

$$-1 \equiv a^2 \mod p$$

Let

$$a \equiv g^l \mod p$$

So

$$-1 \equiv g^{2l} \equiv g^{\frac{p-1}{2}} \mod p$$

The exponents are equivalent, so

$$2l \equiv \frac{p-1}{2} \mod p-1$$

$$l = \frac{p-1}{4}$$

$$4l + 1 = p. \quad p = 1 \mod 4.$$

Now, suppose that $p = 1 \mod 4$.

$$(g^{\frac{p-1}{4}})^2 = g^{\frac{p-1}{2}} \equiv -1 \mod p$$

Since $1 \equiv g^0 \mod p \equiv g^{p-1} \mod p$

$$1 \neq g^{\frac{p-1}{2}^2} \equiv g^{p-1} \equiv 1$$

and thus, -1 is a square. □

Lemma 16. *If -1 is not a square $\mod p$, then a is a square if and only if $-a$ is not a square.*

Proof. Suppose -1 is not a square.
$a = g^k \mod p$ where g is a primitive root.
Since -1 is not a square, then $-1 \equiv g^{2n+1}$ for some n.
So, $-a = g^{k+2n+1}$. Notice that when k is even, $k+2n+1$ is odd and vice-versa, so a and $-a$ have opposite parity.
Thus, if one is a square, then the other is not, and vice-versa. □

Now, we know that -1 is not a square, so we break up $F_p^\times$ into two lists, those that have two roots and those that have none. From previous lemma, if $a \in F_p^\times$ is a square, then $-a \in F_p^\times$ is not a square. Thus, the lists have identical number of elements.

Proposition 17. *n is a congruent number if and only if*

$$\exists P = (x, y) \in E_n(\mathbb{Q}) \quad \textit{such that} \quad y \neq 0.$$

We will prove this later in this paper, but for now, let us take it for granted.

Let $f(x)$ be an odd, non-singular polynomial $\mod p$. Then $f(x) = 0$ has three roots, namely $0, n, -n$.
Then, the total number of elements of $E_n(F_p)$ are $2 \times \frac{p-3}{2}$, the (x, y) with $y \neq 0$ from the lists of squares and non-squares, plus 3 elements with $y = 0$ and finally the point at infinity.

This sums to $2 \times \frac{p-3}{2} + 3 + 1 = p + 1$ total elements.
And thus, we have shown that for $p \equiv 3 \mod 4$ $\#E_n(F_p) = p + 1$. □

Definition 18. The number of linearly independent points of infinite order on E is called the *rank* of E.
Recall that $P_1, \ldots P_k$ are linearly independent if $\sum_{j=1}^{k} n_j P_j = 0 \to n_1 = \ldots = n_k = 0$.

Note: The quotient $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$ is isomorphic to $\mathbb{Z}^r$, where r is the rank of E. Thus, the rank is equal to the sum of linearly independent, non-torsion points.

Example 19. Find the rank of $E(\mathbb{Q}) : y^2 = x^3 - 25x$

$$P = (5, 0), Q = (-5, 0), R = (-4, 6)$$

$$\text{Note that} \quad 2P = \mathcal{O}, \quad 2Q = \mathcal{O}.$$

But

$$2R = (\frac{1681}{44}, \frac{-62279}{1728}), \quad 3R = (\frac{-2439844}{5094049}, \frac{39601568754}{11497268596})$$

One can prove that the rank of this curve is 1 since $nR \nrightarrow \mathcal{O}$.

Example 20. For some higher rank curves, rank is much more difficult to obtain.

For instance, $E(\mathbb{Q}) : y^2 = 4x^3 - 28x + 25$ has a rank of 3.

A quick computation shows that many points on E are have integer coordinates, none of which have $y = 0$. The generators change depending on the chosen set of points, so linear independence is not so easy to define. It is possible to show, although it will not be shown in this paper, that the rank of this curve is 3.

Theorem 21. *If a point $P \in E(\mathbb{Q})$ is non-torsion, then all multiples of P are distinct.*

Proof. We will use proof by contradiction. Assume that there are non-distinct multiples of a point $P \in E(Q)$ such that

$$nP = mP, \quad n > m > 0.$$

$$\text{Then} \quad (n - m)P = 0.$$

Thus, P is $(n - m)$ torsion. □

Note: The current record for highest rank of an elliptic curve was discovered in May 2006 by Noam Elkies of Harvard University. The elliptic curve, which has rank 28, is given by

$$y^2+xy+y = x^3-x^2-20067762415575526585033208209338542750930230312178956502x$$

$$+3448161179503055646703298569039072037485594435931918036 12 \ldots 660082962919394487322434 29.$$

Theorem 22. *n is a congruent number if and only if $E_n(\mathcal{Q})$ has positive rank.*[3]

This result is illustrated by the coefficients of the L-Series. If this L-series vanishes, then then E_n has positive rank. A complete discussion of the L-Series can be found in Koblitz Chapter 2.

[3]A formal proof for this theorem is given in Koblitz, Introduction to Elliptic Curves and Modular Forms, Chapter 1 Proposition 18. This proof relies heavily on our Theorem 13.

2.2 The L-Series

The L-series of an elliptic curve is a product over all primes of the local zeta functions for the elliptic curve.

Definition 23. Local Zeta Function
The local zeta function is a counting object for something defined over F_p.

Example 24. Supose we want to count the number of irreducible prime polynomials modulo p. We can form the following series:

$$Z(T) = \sum_{monic f} T^{deg(f)}$$

For instance, take $f(x) = x^2+ax+b$. This is a degree two polynomial. There are p choices for a and p choices for b, so there are a total of p^2 possible polynomials. So,

$$Z(T) = \sum_{d=0}^{\infty} p^d T^d = \sum_{d=0}^{\infty} pT^d = \frac{1}{1-pT}$$

Note here that $|pT| < 1$ and $|T| < \frac{1}{p}$. Now, every polynomial factors as a product of irreducibles to some powers, such that: $f = g_1^{n_1} \dots g_r^{n_r}$.
Note that

$$deg(f) = n_1 deg(g_1) + \ldots + n_r deg(g_r)$$

So,

$$Z(T) = \sum_{monic f} T^{deg(f)} = \prod_g (1 + T^{deg(g)} + T^{2deg(g)} \dots) = \prod_g (1 - T^{deg(g)})^{-1}$$

Where the product is over irreducible monic polynomial g. Since the factoring is unique, we get an identity between the two series, and we can count the number of irreducible prime polynomials modulo p.
While we will not define the local zeta function or L-series for E, the local zeta function as a counting object is shown by this example.

2.3 The Relationship between elliptic curves and congruent numbers

Proposition 25. *Let n be a rational number. There is a bijection between*

$$A = \{(a,b,c) \in \mathbb{Q}^3 : \frac{ab}{2} = n, \quad a^2+b^2 = c^2\} \quad \textit{and} \quad B = \{(x,y) \in \mathbb{Q}^2 : y^2 = x^3 - n^2 x, \quad y \neq 0\}$$

given by the maps

$$f(a,b,c) = (\frac{-nb}{a+c}, \frac{2n^2}{a+c}) \quad \textit{and} \quad g(x,y) = (\frac{n^2-x^2}{y}, \frac{-2xn}{y}, \frac{n^2+x^2}{y}).$$

Proof.

$$\text{Let} \quad a = \frac{n^2 - x^2}{y}, \quad b = \frac{-2xn}{y}, \quad c = \frac{n^2 + x^2}{y}.$$

$$\text{Then} \quad f(a,b,c) = (\frac{\frac{2xn^2}{y}}{\frac{2n^2}{y}}, \frac{\frac{2n^2}{2n^2}}{\frac{}{y}}) = (x,y).$$

$$\text{Let} \quad x = \frac{-nb}{a+c}, \quad y = \frac{2n^2}{a+c}.$$

$$\text{Then} \quad g(x,y) = (\frac{n^2 - (\frac{-nb}{a+c})^2}{\frac{2n^2}{a+c}}, \frac{\frac{2n^2 b}{a+c}}{\frac{2n^2}{a+c}}, \frac{n^2 + (\frac{-nb}{a+c})^2}{\frac{2n^2}{a+c}}).$$

Simplifying term by term yields

$$a = n^2(1 - \frac{b^2}{(a+c)^2}) \cdot \frac{a+c}{2n^2} = \frac{1}{2}((a+c) - \frac{b^2}{a+c}) = \frac{1}{2}(\frac{a^2 + 2ac + c^2 - b^2}{a+c}).$$

Noting that $a^2 = c^2 - b^2$, we further simplify to

$$\frac{1}{2}(\frac{2a^2 + 2ac}{a+c}) = \frac{1}{2}(2a) = a.$$

The calculation for the second term is easily reduced such that it equals b.

$$c = n^2(1 + \frac{b^2}{(a+c)^2}) \cdot \frac{a+c}{2n^2} = \frac{1}{2}((a+c) + \frac{b^2}{a+c}) = \frac{1}{2}(\frac{a^2 + 2ac + c^2 + b^2}{a+c}).$$

Noting that $c^2 = a^2 + b^2$, we further simplify to

$$\frac{1}{2}(\frac{2c^2 + 2ac}{a+c}) = \frac{1}{2}(2c) = c.$$

$$\text{Thus,} \quad g(x,y) = (a,b,c) \quad \text{and} f(a,b,c) = (x,y)$$

So there is a bijection between this two maps. □

We now can return to Proposition 17 to give a clear proof.

Proposition 26. *n is a congruent number if and only if*

$$\exists P = (x,y) \in E_n(\mathbb{Q}) \quad \textit{such that} \quad y \neq 0.$$

Proof. We say that n is a congruent number if and only if $A \neq \emptyset$. Since the sets A and B are bijective, we know that A is non-empty if and only if B is non-empty. □

Now that we have established a bijection between the two sets, let's take a look at an example.

Example 27. Using this bijection, we show that $n = 5$ is a congruent number.

$$\text{Define} \quad E_n(\mathbb{Q}) : y^2 = x^3 - 25x, \quad P = (-4, 6) \in \mathbb{Q}.$$

$$\text{Then} \quad g(-4,6) = (\frac{5^2 - (-4)^2}{6}, \frac{-2 \cdot -4 \cdot 5}{6}, \frac{5^2 + ((-4)^2}{6}) = (\frac{3}{2}, \frac{20}{3}, \frac{41}{6}).$$

This represents the sides of the rational triangle,

$$A = \frac{1}{2}(\frac{3}{2})(\frac{20}{3}) = 5$$

Thus, n is a congruent number.

Finally, with this in mind, we move to Tunnel's Theorem. This powerful theorem gives us a method of computing if a number is a congruent number or not. Tunnel's Theorem relies on the Birch and Swinnerton-Dyer conjecture, which is one of the seven Clay Institute million dollar problems. The theorem is as follows:

Theorem 28. *(Tunnell): Let n be an odd squarefree natural number. Consider the two conditions:*
1) n is congruent.
2) the number of triples of integers (x, y, z) satisfying $2x^2 + y^2 + 8z^2 = n$ is equal to twice the number of triples satisfying $2x^2 + y^2 + 32z^2 = n$.

Then 1 implies 2, and if a weak form of the Birch-Swinnerton-Dyer conjecture is true, then 2 also implies 1.

The Birch-Swinnerton Dyer conjecture relates the coefficients of the L-series (of modular form) to the rank of the elliptic curve. Then, Tunnell's Theorem relates the rank of the elliptic curve to the sides of the rational triangle, given by the bijection shown in Proposition 25. Once that is achieved, it is easy to take an area of the rational triangle and check if the triangle has an area equal to a congruent number.

Example 29. Use Tunnell's Theorem to show that $n = 1$ is not a congruent number.

$$E_n(\mathbb{F}) : y^2 = x^3 - x.$$

The only triple of integers that satisfies $2x^2 + y^2 + 8z^2 = 1$ is $(0, 1, 0)$. Similarly, the only triple of integers that satisfies $2x^2 + y^2 + 32z^2 = 1$ is $(0, 1, 0)$.
Using Tunnell's Theorem, condition 2 is not satisfied, so condition 1 cannot be satisfied. Thus, 1 is not a congruent number.

Since Tunnell's Theorem gives us the coefficients of the L-Series and the second condition is not satisfied, the L-Series indicates that the Ellptic Curve does not have positive rank. By theorem 22, this indicates that $n = 1$ cannot be a congruent number. This theorem gives a clear, precise way to relate elliptic curves and rational triangles.

References

[1] Brad Groff: Congruent Numbers, the Rank of Elliptic Curves and the Birch and Swinnerton-Dyer Conjecture (November 2001) URL: https://www2.bc.edu/ reederma/congruent.pdf

[2] N. Koblitz: Introduction To Elliptic Curves And Modular Forms (Springer-Verlag, 1984).

[3] William Stein: Elementary Number Theory, to appear with Springer, (March-2007). URL: http: //modular.math.washington.edu/papers/. 795